# Cryptography and Network Security

## Block Cipher Modes of Operation

nesoacademy.org

## Outcomes

Upon the completion of this session, the learner will be able to

- ★ Understand the need for block cipher modes of operation.
- ★ Know how does the block cipher work in real time.
- ★ Know the various block cipher modes of operations.

## Need for Modes of Operation

Plaintext 1:

Computer

Plaintext 2:

A lengthy message,

Image file,

Multimedia file,

Real time data etc.,

## Block Cipher

- ★ We don't just 'run a cipher' - we need a mode of operation.
- ★ Fixed-length block.
- ★ 'b' bits input and 'b' bits output.
- ★ If the amount of PT to be encrypted is > 'b' bits?
- ★ Breaking the plaintext into 'b' bits in each block.
- ★ 5 modes of operation defined by NIST.
- ★ Does security issue arise when multiple blocks are encrypted?
- ★ Different applications – Different modes of operation.

## Modes of Operation

- ★ Electronic Codebook (ECB).
- ★ Cipher Block Chaining (CBC).
- ★ Cipher Feedback (CFB).
- ★ Output Feedback (OFB).
- ★ Counter (CTR).

# Cryptography and Network Security

Modes of Operation
Electronic Codebook (ECB)

## Block Cipher Modes of Operation

### 🎯 Outcomes

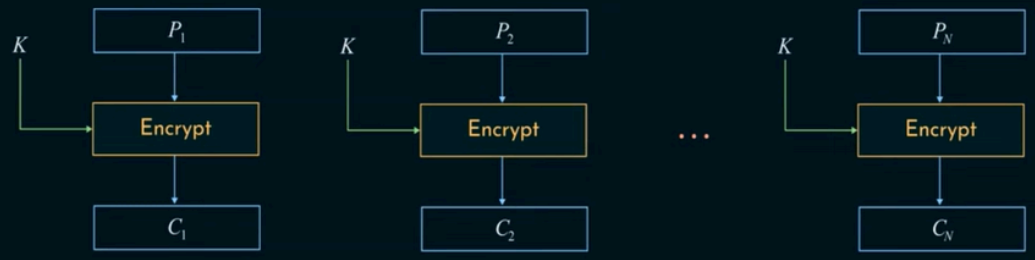
Upon the completion of this session, the learner will be able to

- ★ Understand the ECB mode of operation.
- ★ Know the pros and cons of ECB.
- ★ See an encrypted image to witness the drawback of ECB.

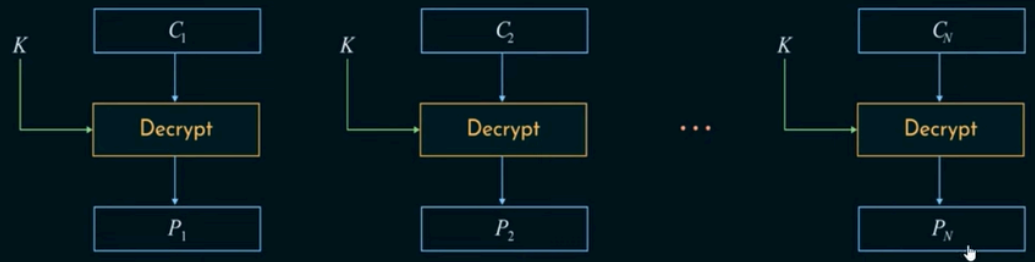
## Electronic Codebook (ECB)

- ★ One plaintext block.
- ★ Each block is encoded independently using the same key.
- ★ Why the term 'codebook'?

# Electronic Codebook (ECB)




ECB - Encryption




ECB - Decryption



# Electronic Codebook (ECB)

**Pros**

- ★ Simplest mode.
- ★ Ideal for short amount of data. Ex: secure transfer of AES or DES key.
- ★ Independent - Can encrypt any block.
- ★ Fast – Parallelism.

**Cons**

- ★ Not secure for lengthy messages.
- ★ Cryptanalyst can exploit the regularities of the message.

## Electronic Codebook (ECB)

Original Image

Encrypted using ECB

Encrypted using other modes

# Cryptography and Network Security

## Modes of Operation
## Cipher Block Chaining (CBC)

nesoacademy.org

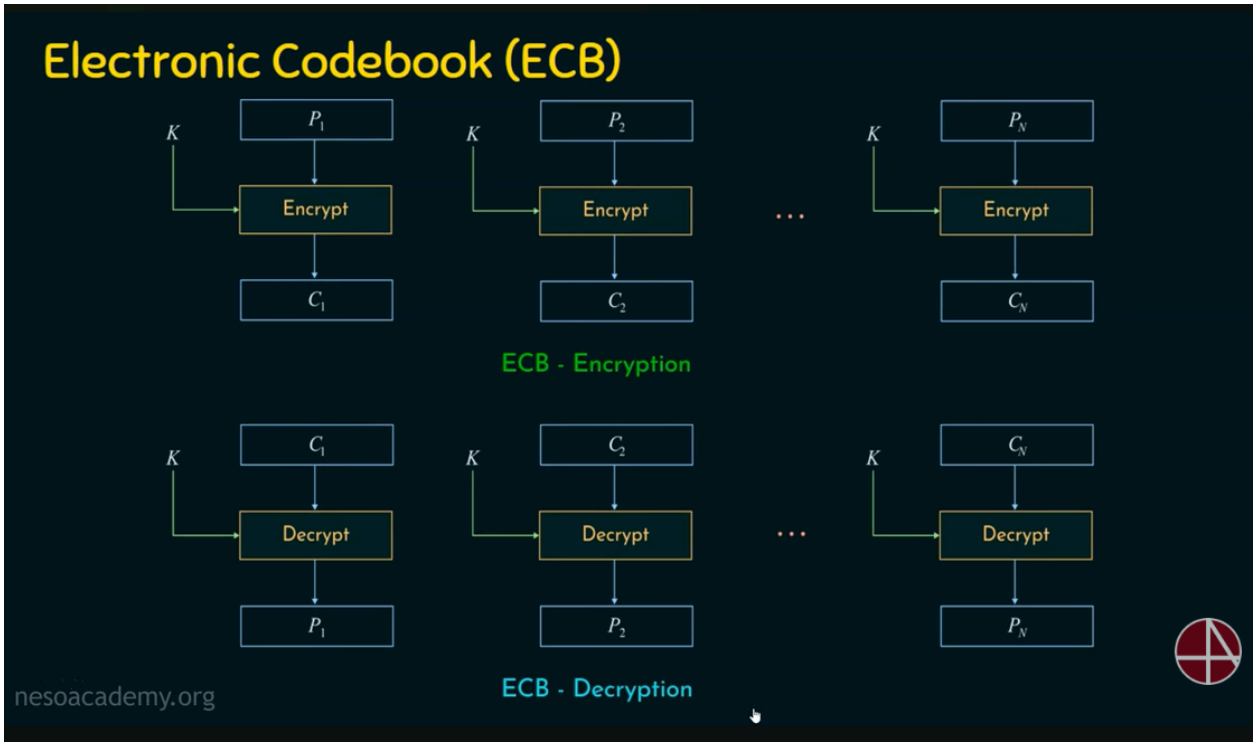
## Outcomes

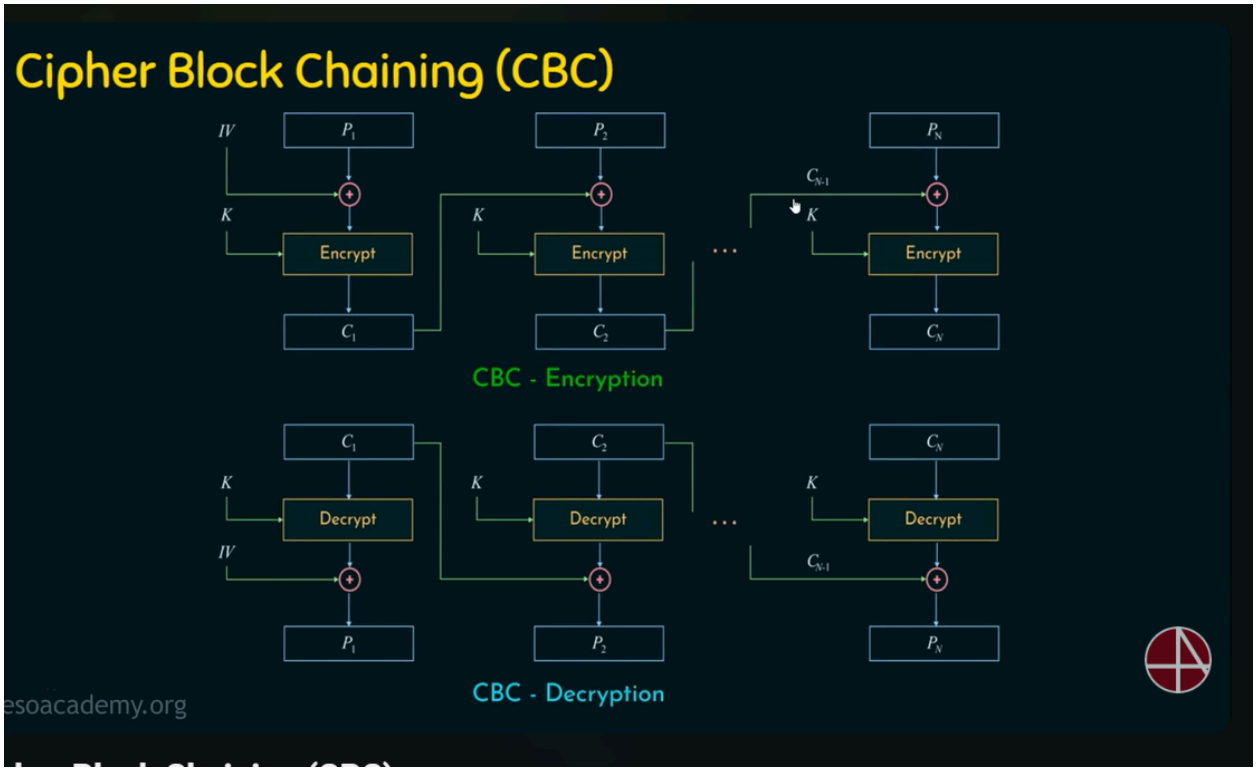
Upon the completion of this session, the learner will be able to

- ★ Recall the security deficiencies of ECB.
- ★ Understand the operation for CBC.
- ★ Understand the pros and cons of CBC.

## Cipher Block Chaining (CBC)

- ★ ECB – Same PT block – Same CT block.
- ★ CBC – Same PT block – Different CT block.
- ★ Same key.
- ★ Chaining.
- ★ Dependent block.
- ★ Therefore, repeating patterns of bits are not exposed.
- ★ General-purpose block oriented transmission.


Electronic Codebook (ECB)
K
$P_1$
Encrypt
$C_1$
$P_2$
$C_2$
$P_N$
$C_N$
ECB - Encryption
$C_1$
Decrypt
$P_1$
$C_2$
$P_2$
$C_N$
$P_N$
nesoacademy.org
ECB - Decryption


Cipher Block Chaining (CBC)
IV
K
$P_1$
Encrypt
$C_1$
$P_2$
$C_2$
$P_N$
$C_{N-1}$
$C_N$
CBC - Encryption
Decrypt
esoacademy.org
CBC - Decryption

## Cipher Block Chaining (CBC)

Pros

- ★ Appropriate mode for encrypting messages of length greater than 'b' bits.
- ★ Confidentiality + Authentication.

Cons

- ★ Slow – No parallelism.
- ★ Cannot encrypt any block since we need the ciphertext of previous block.
- ★ Initialization Vector (IV) which must be known to sender & receiver.

# Cryptography and Network Security

Modes of Operation

Cipher Feedback (CFB)

nesoacademy.org

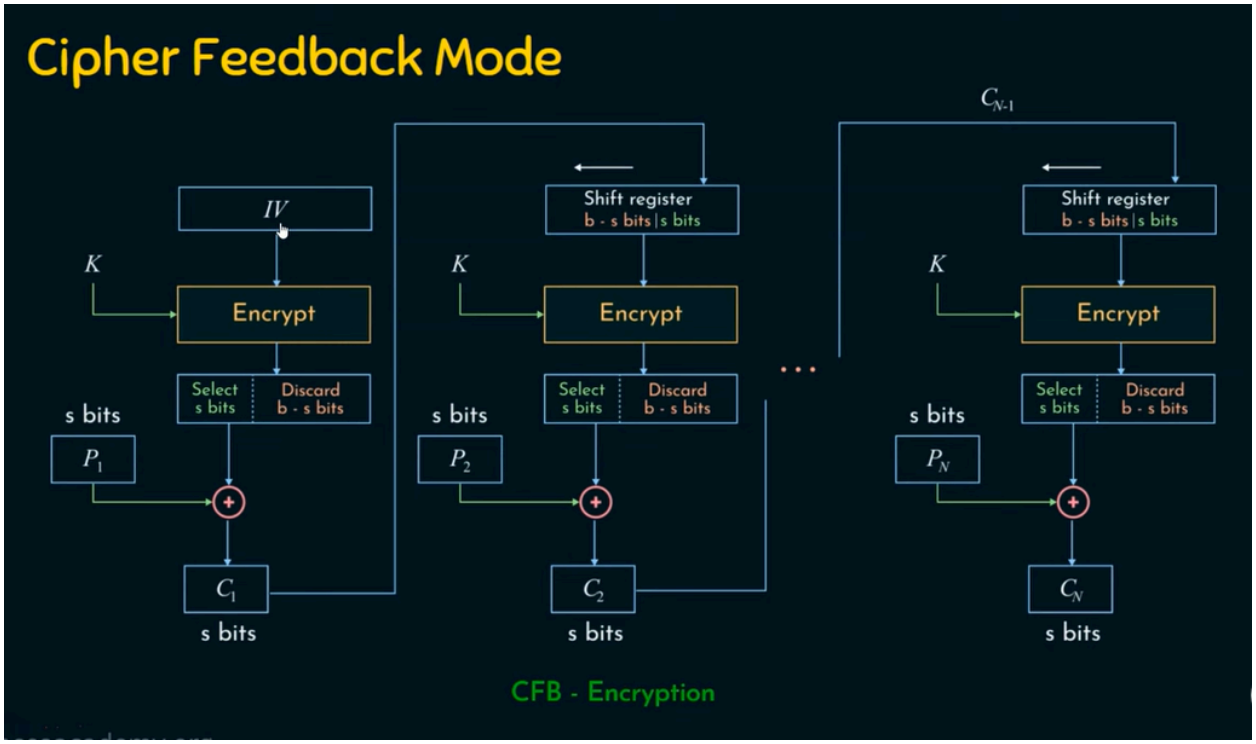
## Outcomes

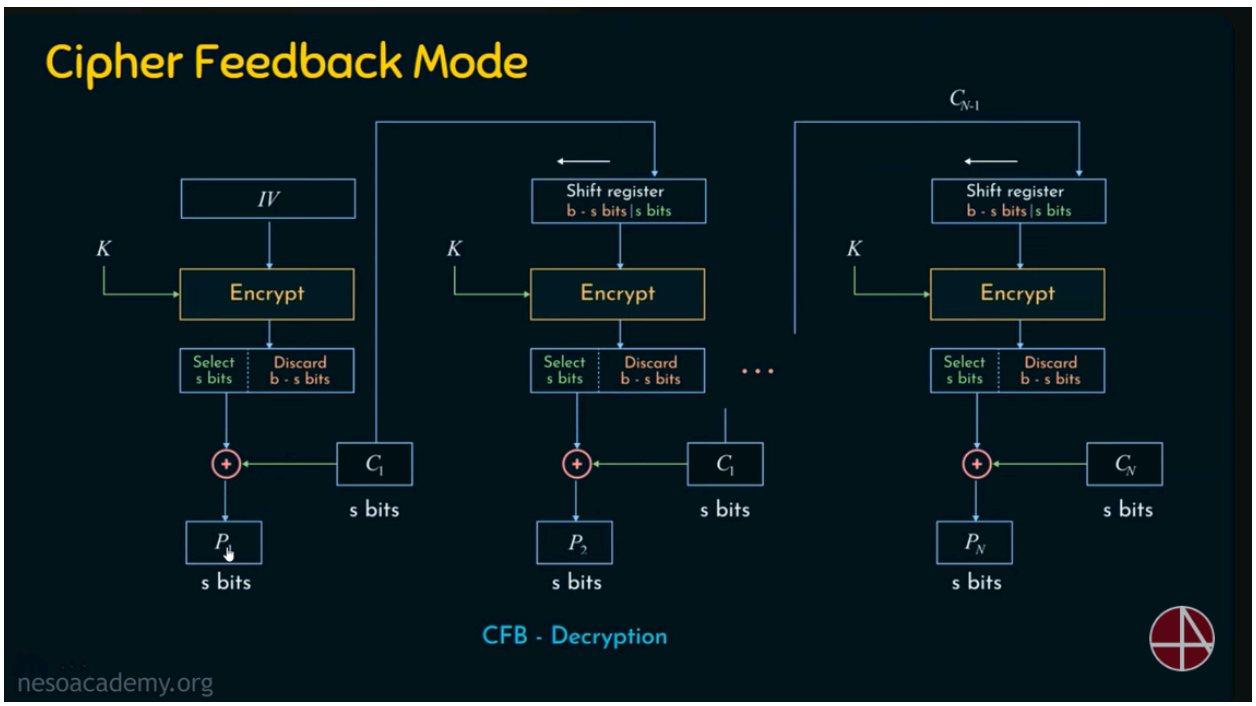
Upon the completion of this session, the learner will be able to

- ★ Understand the need for having stream cipher.
- ★ Understand the working of CFB.
- ★ Know the pros and cons of CFB.

## Cipher Feedback Mode

- ★ Convert a block cipher to stream cipher.
- ★ Why stream cipher?
  - ★ No need of padding.
  - ★ Real time.
  - ★ Length of plaintext = Length of ciphertext.
- ★ General-purpose stream oriented transmission.
- ★ Authentication.


Cipher Feedback Mode
$C_{N-1}$
IV
K
Encrypt
Shift register
b - s bits | s bits
Select
s bits
Discard
b - s bits
s bits
$P_1$
$P_2$
$P_N$
$C_1$
$C_2$
$C_N$
s bits
CFB - Encryption


Cipher Feedback Mode
$C_{N-1}$
IV
K
Encrypt
Shift register
b - s bits | s bits
Select
s bits
Discard
b - s bits
$C_1$
$C_N$
s bits
$P_1$
$P_2$
$P_N$
CFB - Decryption
nesoacademy.org

# Cipher Feedback Mode

Pros

- ★ Can operate in real time.
- ★ Need of padding is eliminated.
- ★ Encryption function does decryption as well.
- ★ Length of PT = Length of CT.

Cons

- ★ Chances of wastage of transmission capacity.
- ★ Not a typical stream cipher.

# Cryptography and Network Security

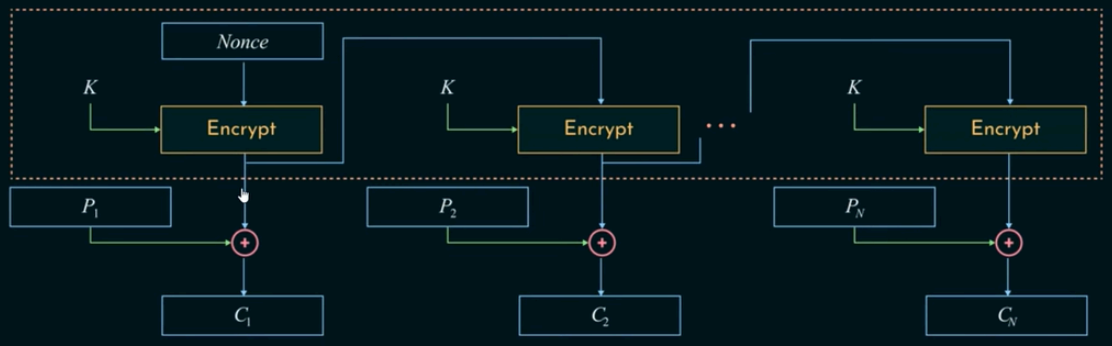
## Modes of Operation
## Output Feedback (OFB)

# Outcomes

Upon the completion of this session, the learner will be able to

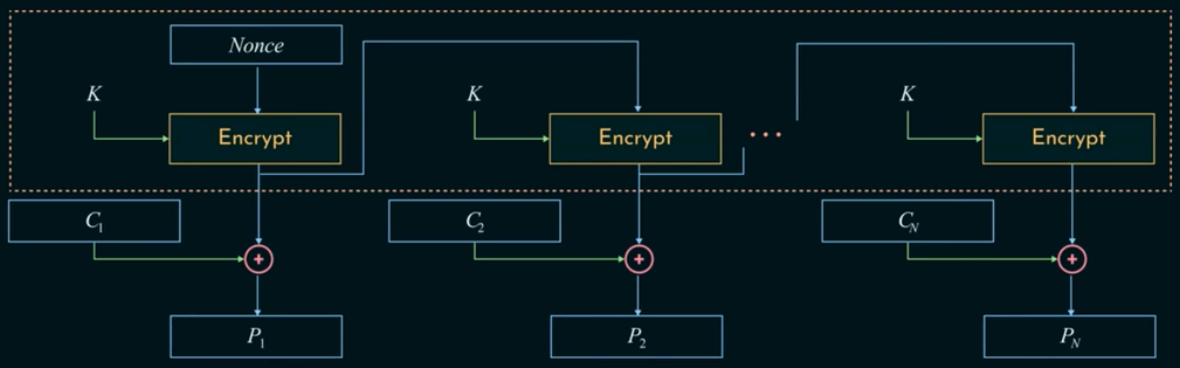
- ★ Understand the encryption and decryption of OFB.
- ★ Know the difference of working of OFB from CFB.
- ★ Know the pros and cons of OFB.

# Output Feedback




OFB - Encryption

# Output Feedback




OFB - Decryption

# Output Feedback

**Pros:**

- ★ Bit errors in transmission do not propagate.
- ★ Same PT – Same Key – Different CT.
- ★ The PT length can be of random choice.

**Cons:**

- ★ Sender and Receiver must be synced.
- ★ More vulnerable to modification attack.
- ★ No parallelizable.
- ★ IV and keys must be regenerated every time.

# Cryptography and Network Security

## Modes of Operation
## Counter Mode (CTR)

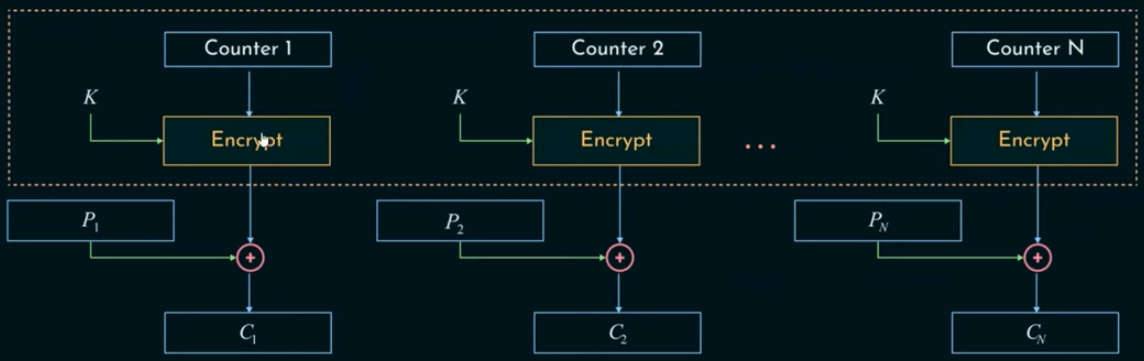
nesoacademy.org

## Counter Mode

- ★ Applications to ATM, IP Sec etc.,
- ★ Counters.
- ★ Size of counter = plaintext block size.
- ★ Different counter value for each plaintext.
- ★ Counter value is initialized.
- ★ Counter++.
- ★ Decryption - Same sequence of counter values is used.
- ★ Decryption - Initial value of counter is made available.
- ★ What about for last block?

nesoacademy.org

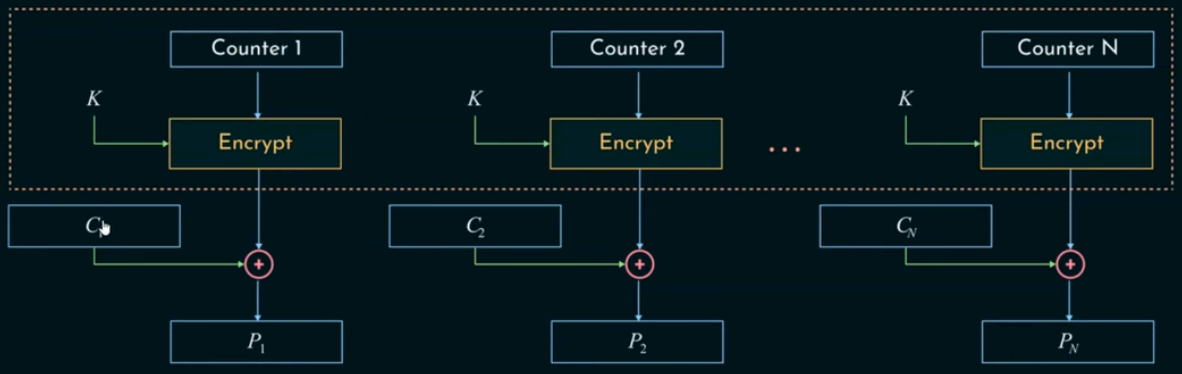
# Counter Mode




CTR - Encryption



# Counter Mode




CTR - Decryption

# Counter Mode

## Advantages

- ★ Hardware efficiency.
- ★ Software efficiency.
- ★ Preprocessing.
- ★ Random access.
- ★ Provable security.
- ★ Simplicity.

## Question

Consider the CFB mode of operation where the block cipher is permutation cipher and key is a permutation $\begin{matrix}1 & 2 & 3 & 4\\ 3 & 4 & 2 & 1\end{matrix}$.

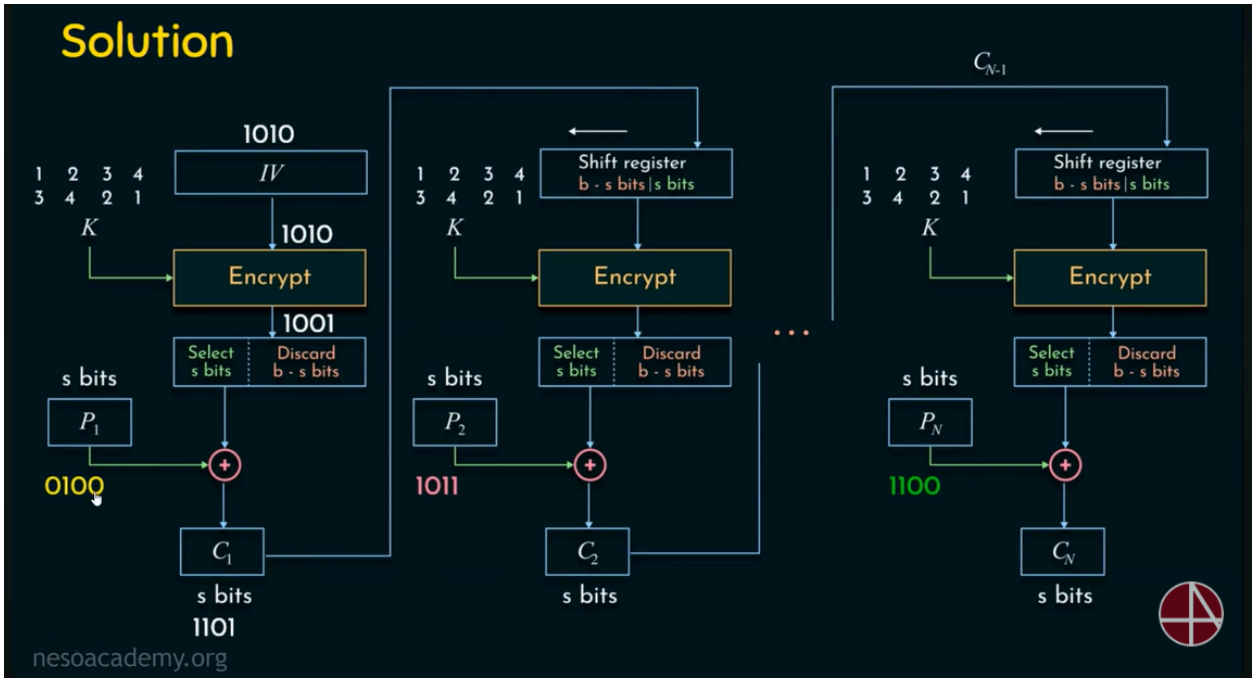
If the IV is taken as 1010 then what is the corresponding ciphertext corresponding for the plaintext 010010111100?

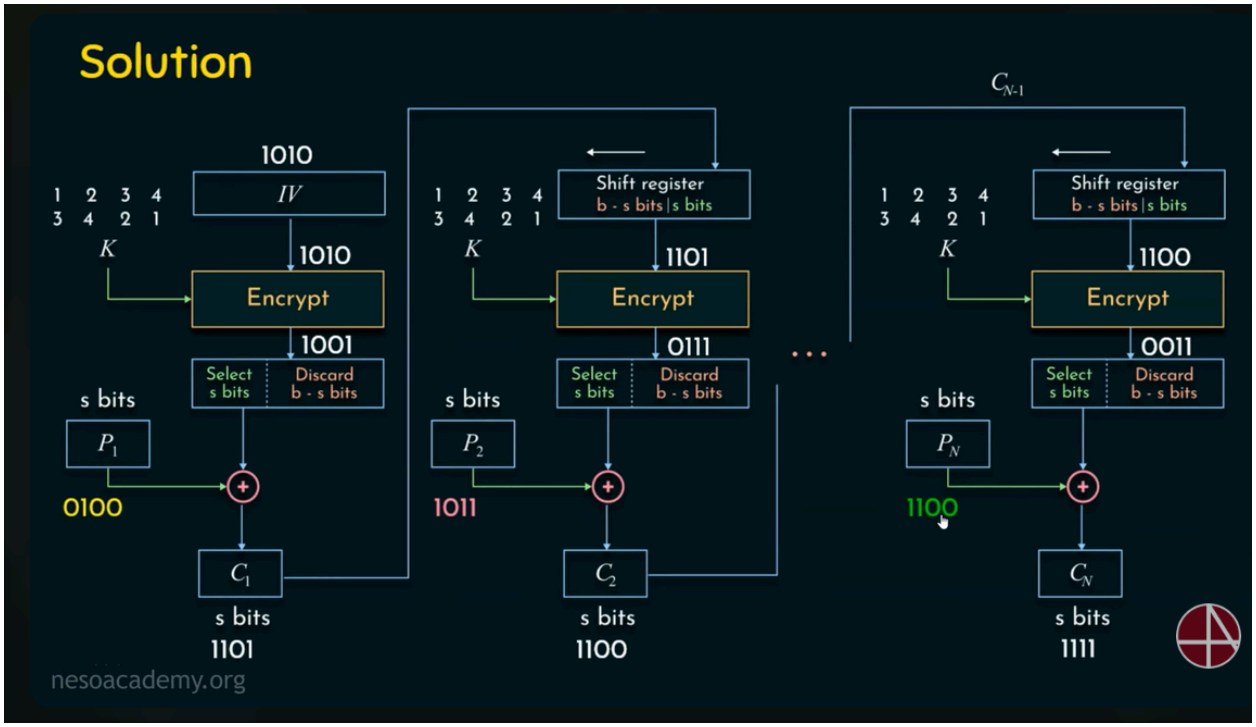
a. 110100111100

b. 110100111010

c. 110111100011

d. 110111001111


Solution
1010
IV
1 2 3 4
3 4 2 1
K
1010
Encrypt
1001
Select s bits
Discard b - s bits
s bits
P1
0100
C1
s bits
1101
Shift register
b - s bits | s bits
P2
1011
C2
CN-1
PN
1100
CN
nesoacademy.org


Solution
1010
IV
1 2 3 4
3 4 2 1
K
1010
Encrypt
1001
Select s bits
Discard b - s bits
s bits
P1
0100
C1
s bits
1101
Shift register
b - s bits | s bits
1101
0111
P2
1011
C2
1100
CN-1
1100
0011
PN
1100
CN
1111
nesoacademy.org